arXiv:1203.4077v1 [cs.CR] 19 Mar 2012

A DIGITAL SIGNATURE SCHEME FOR LONG-TERM SECURITY

DIMITRIOS POULAKIS AND ROBERT ROLLAND

Abstract. In this paper we propose a signature scheme based on two intractable problems, namely the integer factorization problem and the discrete logarithm problem for elliptic curves. It is suitable for applications requiring long-term security and provides a more efficient solution than the existing ones.

1. Introduction

Many applications of the Information Technology, such as encryption of sensitive medical data or digital signatures for contracts, need long term cryptographic security. Unfortunately, today's cryptography provides strong tools only for short term security [5]. Especially, digital signatures do not guarantee the desired long-term security. In order to achieve this goal Maseberg [17] suggested the use of more than one sufficiently independent signature schemes. Thus, if one of them is broken, then it can be replaced by a new secure one. Afterward the document has to be re-signed. Again we have more than one valid signatures of our document. Of course, a drawback of the method is that the document has to be re-signed.

In order to avoid this problem, it may be interesting for applications with long-term, to base the security of cryptographic primitives on two difficult problems, so if any of these problems is broken, the other will still be valid and hence the signature will be protected. We propose in this paper a signature scheme built taking into account this constraint. The following signature scheme is based on the integer factorization problem and the discrete logarithm problem on a supersingular elliptic curve. Remark that these two problems have similar resistance to attack, thus they can coexist within the same protocol. The use of a supersingular curve allows us to easily build a pairing that we use to verify the signature. Note that our system is the first one that combines these two problems.

Signature schemes combining the intractability of the integer factorization problem and integer discrete logarithm problem were proposed but most of them have proved to be not as secure as claimed [6, 8, 14, 15, 16, 19, 23].

In section 2 we describe the infrastructure for the implementation of the scheme. Then we present the key generation, the generation of a signature and the verification. In section 3 we study the security of the scheme. In section 4 we show how to build a elliptic curve adapted to the situation and how to define a valuable pairing on it. In section 5 we address the problem of the map to point function and give

Date: February 27, 2013.

2000 *Mathematics Subject Classification.* Primary 94A62; Secondary 11T71, 94A60, 14G50.

Key words and phrases. Digital signature ; Integer factorization; Elliptic curve discrete logarithm; Supersingular elliptic curves; Pairing; Map to point function; Long-term security.

a practical solution. In section 7 we give a complete example that shows that the establishment of such a system can be made in practice.

2. The Proposed Signature Scheme

In this section we present our signature scheme.

2.1. **Public and private key generation.** A user $\mathcal{A}$, who wants to create a public and a private key selects:

(1) primes p_1 and p_2 such that the factorization of $n = p_1p_2$ is infeasible;
(2) an elliptic curve E over a finite field $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ with $\text{ord}(P) = n$ and an efficiently computable pairing e_n such that $e_n(P, P)$ is a primitive n-th root of 1;
(3) three integers $g \in \{1, \dots, n-1\}$ with $\gcd(g, n) = 1$ and $a, b \in \{1, \dots, \phi(n)-1\}$ and computes $Q = g^aP$, $r = g^b \pmod n$ and $R = g^{a-ab}P$;
(4) two hash functions, $H : \{0,1\}^* \to < P >$, where $< P >$ is the subgroup of $E(\mathbb{F}_q)$ generated by P, and $h : \{0,1\}^* \to \{0, \dots, n-1\}$.

$\mathcal{A}$ publishes the elliptic curve E, the pairing e_n and the hash functions h and H. The public key of $\mathcal{A}$ is (g, P, Q, R, r, n) and his private key (a, b, p_1, p_2).

2.2. **Signature generation.** $\mathcal{A}$ wants to sign a message $m \in \{0,1\}^*$. Then he computes

$$S = g^{ab}H(m)$$

and

$$s = bh(m) + a - ab \bmod \phi(n).$$

Let $x(S)$ be the x-coordinate of S. The signature of m is the couple $(x(S), s)$.

2.3. **Verification.** Suppose that (x, s) is the signature of m. The receiver determines y such that $\Sigma = (x, y)$ is a point of $E(\mathbb{F}_q)$. He accepts the signature if and only if

$$e_n(\pm g^s\Sigma, P) = e_n(r^{h(m)}H(m), Q)$$

and

$$g^sP = r^{h(m)}R.$$

Proof of correctness of verification. Suppose that the signature (x, s) is valid and $\Sigma = (x, y)$ is a point of $E(\mathbb{F}_q)$. Then $\Sigma = \pm S$ and so, we get

$$e_n(\pm g^s\Sigma, P) = e_n(g^sS, P) = e_n(g^{bh(m)+a-ab}g^{ab}H(m), P) = e_n(r^{h(m)}H(m), Q)$$

and

$$g^sr^{-h(m)}P = g^{h(m)b+a-ab}g^{-bh(m)}P = g^{a-ab}P = R.$$

Suppose now we have a couple (S, s) such that

$$e_n(g^sS, P) = e_n(r^{h(m)}H(m), Q), \quad g^sP = r^{h(m)}R.$$

Since $H(m), S \in < P >$, there are $u, v \in \{0, \dots, n-1\}$ such that $S = uP$ and $H(m) = vP$. Then we get

$$e_n((g^su - r^{h(m)}vg^a)P, P) = 1.$$

The element $e_n(P, P)$ is a primitive n-th root of 1 and so, we obtain

$$g^su \equiv r^{h(m)}g^av \pmod n$$

whence

$$uv^{-1} \equiv r^{h(m)} g^{-s} g^a \equiv g^{-s+bh(m)+a} \pmod{n}.$$

On the other hand, the equality

$$g^s P = r^{h(m)} R$$

implies

$$g^{s-bh(m)} \equiv g^{a-ab} \pmod{n}$$

and so, we get

$$uv^{-1} \equiv g^{ab} \pmod{n}.$$

Hence, we obtain

$$s = bh(m) + a - ab \bmod \phi(n), \quad S = g^{ab} H(m),$$

whence we have that $(x(S), s)$ is a signature for m.

3. Security

We remark that if an attacker wants to compute a and b from the public key, he has to compute either the discrete logarithm of Q and R to the base P and next to calculate a discrete logarithm modulo n or to compute the discrete logarithm of r to the base g, the discrete logarithm of one of Q and R to the base P, and next a discrete logarithm modulo n. Thus, he has to compute at least a discrete logarithm in the group $< P >$ and two logarithms modulo n. Note that an algorithm which computes the discrete logarithm modulo n implies an algorithm which breaks the Composite Diffie-Hellman key distribution scheme for n and any algorithm which break his scheme for a non negligible proportion of the possible inputs can be used to factorize n [18, 2].

Let $p(d, a)$ be the smallest prime of the arithmetic progression $\{a + kd/k \geq 0\}$. Put

$$p(d) = \max\{p(d, a)/\ 1 \leq a < d,\ \gcd(a, d) = 1\}.$$

In 1978, Heath-Brown [9] conjectured that $p(d) < Cd(\log d)^2$. We shall use this conjecture in order to show that we can construct a supersingular elliptic curve having a subgroup of order n in polynomial time.

We consider the arithmetic progression $4nj + 4n - 1$ $(j = 0, 1, 2, \ldots)$. The above conjecture implies that there exists a prime $q < C4n(\log 4n)^2$ such that $q \equiv 4n - 1 \pmod{4n}$. Hence there is $j < C(\log 4n)^2$ such that $q = 4nj + 4n - 1$, whence $q + 1 = 4n(j + 1)$. Thus, we can find the prime q in polynomial time, using a primality test $O((\log n)^2)$ times. Moreover, since $q \equiv 3 \pmod 4$, the elliptic curve $y^2 = x^3 + x$ on $\mathbb{F}_q$ is supersingular.

Suppose now there is an oracle $\mathcal{O}$ such that given a public key and a message m provides a signature for m.

Let n be an integer which is the product of two (unknown) primes. We shall use the oracle $\mathcal{O}$ in order to factorize n. Let E be an elliptic curve as above and a point $P \in E(\mathbb{F}_q)$ of order n. Furthermore, we consider $g, a, b \in \{1, \ldots, n-1\}$ and we compute $r = g^b \bmod n$, $Q = g^a P$ and $R = g^{a-ab} P$. So, we have the public key (g, P, Q, R, r, n) for our system. Then $\mathcal{O}$ gives signatures (S_i, s_i) for the messages m_i $(i = 1, \ldots, k)$ and so, we have $s_i = bh(m_i) + a - ab \bmod \phi(n)$. It follows that $\phi(n)$ divides the gcd d of the number $s_i - bh(m_i) - a + ab$ $(i = 1, \ldots, k)$ and hence $\phi(n)$ is among the divisors of d. Note however that, assuming the numbers $s_i - bh(m_i) - a + ab$ follow the uniform distribution, the probability that two such

numbers has gcd $> \phi(n)$ is quite small. Thus, $\phi(n)$ can be easily computed and so the factorization of n.

Let G_1 and G_2 be two (multiplicative) cyclic groups of prime order p; g_1 is a fixed generator of G_1 and g_2 is a fixed generator of G_2; ψ is an isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. We recall the following problem [3].

Computational co-Diffie - Hellman on (G_1, G_2). Given γ_2, $\gamma_2^{\alpha} \in G_2$ and $h \in G_1$ as input, compute $h^{\alpha} \in G_1$.

The best known algorithm for solving the above problem is to compute discrete logarithm in G_1.

Assuming that p_1 and p_2 are known, we consider $P_i \in E(\mathbb{F}_q)$ with order p_i. We take $g_i \in \{1, \dots, p_i - 1\}$ and $a, b \in \{1, \dots, \phi(n)\}$ and we compute $Q_i = g_i^a P_i$, $R_i = g_i^{a-ab} P_i$ and $r_i = g_i^b \bmod p_i$ $(i = 1, 2)$.

Let $g, r \in \{1, \dots, n-1\}$ such that $g \equiv g_i \pmod{p_i}$, $r \equiv r_i \pmod{p_i}$, $(i = 1, 2)$. We set $P = P_1 + P_2$, $Q = Q_1 + Q_2$ and $R = R_1 + R_2$. Thus

$$Q = Q_1 + Q_2 = g_1^a P_1 + g_2^a P_2 = g^a P$$

and

$$R = R_1 + R_2 = g_1^{a-ab} P_1 + g_2^{a-ab} P_2 = g^{a-ab} P.$$

Therefore, (g, P, Q, R, r, n) is a public key for our signature scheme.

We apply $\mathcal{O}$ on (g, P, Q, R, r, n) and $m \in \{0,1\}^*$, and we get the signature (S, s) for m. Thus, we have $S = g^{ab} H(m)$, whence it follows $g^s r^{-h(m)} S = g^a H(m)$. Set $S = S_1 + S_2$ and $H(m) = H_1 + H_2$, where $S_i, H_i \in < P_i >$ $(i = 1, 2)$. Then, we have $g_i^s r_i^{-h(m)} S_i = g_i^a H_i$, and so, $g_i^s r_i^{-h(m)} S_i$ is the solution of the computational problem co-Diffie-Hellman with $\gamma_2 = P_i$, $\alpha = g_i^a$ and $h = H_i$ $(i = 1, 2)$.

4. The elliptic curve and the pairing

In this section we show how we can construct an elliptic with the desired properties in order to implement our signature scheme. This task is achieved by the following algorithm:

(1) select two large prime numbers p_1 and p_2 such that the factorization of $p_1 - 1$, $p_2 - 1$ are known and the computation of the factorization of $n = p_1 p_2$ is infeasible;
(2) select a random prime number p and compute $m = \mathrm{ord}_n(p)$;
(3) find, using the algorithm of [4], a supersingular elliptic curve E over $\mathbb{F}_{p^{2m}}$ with trace $t = 2p^m$;
(4) return $\mathbb{F}_{p^{2m}}$ and E.

Since the trace of E is $t = 2p^m$, we get $|E(\mathbb{F}_{p^{2m}})| = (p^m - 1)^2$. On the other hand, we have $m = \mathrm{ord}_n(p)$, whence $n | p^m - 1$, and so n is a divisor of $|E(\mathbb{F}_{p^{2m}})|$. Therefore $E(\mathbb{F}_{p^{2m}})$ contains a subgroup of order n.

By [4, Theorem 1.1], we obtain, under the assumption that the Generalized Riemman Hypothesis is true, that the time complexity of Step 3 is $\tilde{O}((\log p^{2m})^3)$. Furthermore, since the factorization of $\phi(n) = (p_1 - 1)(p_2 - 1)$ is known, the time needed for the computation of m is $O((\log n)^2 / \log\log n)$ [13, Section 4.4].

For the implementation of our signature scheme we also need a point P with order n and an efficiently computable pairing e_n such that $e_n(P, P)$ is a primitive n-th root of 1. The Weil pairing does not fulfill this requirement and also, in many

instances, the Tate pairing; the same happens for the eta, ate or omega pairings [1, 10, 22]. Let ϵ_n be one of the previous pairings on $E[n]$. Following the method introduced by E. Verheul [20], we use a distortion map ϕ such that the points P and $\phi(P)$ is a generating set for $E[n]$ and we consider the pairing $e_n(P,Q) = \epsilon_n(P, \phi(Q))$. The algorithm of [7, Section 6] provides us a method for the determination of P and ϕ.

Another method for the construction of the elliptic curve E which is quite efficient in practice is given by the following algorithm:

(1) draw at random a prime number p_1 of a given size l (for example l is 1024 bits);
(2) draw at random a number p_2 of size l;
(3) repeat $p_2 = \text{NextPrime}(p_2)$ until $4p_1p_2 - 1$ is prime;
(4) return $p = 4p_1p_2 - 1$.

It is not proved that this algorithm will stop with a large probability. This is an open problem which is for $p_1 = 2$ the Sophie Germain number problem. But in practice we obtain a result p which is a prime of length $2l$.

Since $p \equiv 3 \mod 4$, the elliptic curve defined over $\mathbb{F}_p$ by the equation

$$y^2 = x^3 + ax,$$

where $-a$ is not a square in $\mathbb{F}_p$, is supersingular with $p + 1 = 4p_1p_2$ points. By [21, Theoreme 2.1], the group $E(\mathbb{F}_p)$ is either cyclic or $E(\mathbb{F}_p) \simeq \mathbb{Z}/2p_1p_2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In each case the group $E(\mathbb{F}_p)$ has only one subgroup of order $n = p_1p_2$, and this subgroup is cyclic.

If ϵ_n is one of the previous pairings on $E[n]$, then we use the distorsion map $\phi(Q) = \phi(x, y) = (-x, iy)$ with $i^2 = -1$ (cf. [11]) and so, we obtain the following pairing: $e_n(P,Q) = \epsilon_n(P, \phi(Q))$.

5. The map to point function

Let G be the subgroup of order $n = p_1p_2$ of $E(\mathbb{F}_q)$ introduced in the previous section. In order to sign using the discrete logarithm problem on this group, we have to define a hash function into the group G, namely a map to point function. This problem was studied by various authors giving their own method, for example in [3] or [12]. We give here the following solution. Let us denote by $|n| = \lfloor \log_2(n) \rfloor + 1$ the size of n. Let h be a key derivation function, possibly built using a standard hash function. We recall that h maps a message M and a bitlength l to a bit string $h(M, l)$ of length l. Moreover we will suppose that h acts as a good pseudo-random generator. Let Q be a generator of the group G. Let us denote by $(T_i)_{i \geq 0}$ the sequence of bit strings defined by $T_0 = 0$ and for $i \geq 1$

$$T_i = a_u \cdots a_0,$$

where $i = \sum_{j=0}^{u} a_j 2^j$ and $a_u = 1$.

To map the message m to a point $H(m)$ we run the following algorithm:

$i := 0$;
Repeat
  $k := h(m||T_i, |n|)$;
  $i := i + 1$;
Until $k < n$;

Output $H(M) = k.Q$;

This Las Vegas algorithm has a probability zero to never stop. In pratice this algorithm stops quickly, namely as $2^{|n|-1} < n < 2^{|n|}$ then the expected value of the number of iterations is < 2. If one can find a collision for H it is easy to find a collision for h.

6. Performance Analysis

In this section we analyze the performance of our scheme. The computation of s requires the computation of the hash value $h(m)$, two modular multiplications $bh(m), ab \pmod{\phi(n)}$, and finally a modular subtraction. The computation of S needs a modular exponentiation $g^{ab} \pmod{n}$ and the computations of $H(m)$ and $g^{ab}H(m)$. Note that the computations of $a - ab \pmod{\phi(n)}$ and $g^{ab} \pmod{n}$ can be done off-line. Thus, the signature generation requires only the computation of the hash values $h(m)$, $H(m)$, a modular multiplication, a modular addition and a point multiplication on the elliptic curve. Hence, we see that the signature generation algorithm for our scheme is quite fast.

The signature verification needs two modular multiplications, four points multiplications on the elliptic curves, two pairing computations and the computations of the hash values.

7. Example

In this section we give an example of our scheme. We consider the 256-bits primes

$$p_1 = 664810154161090130922129022943767028$$
$$357741958992075598068605416695786374942 31$$

and

$$p_2 = 115738576089152909314582339834842248600$$
$$964273864643984203082855344579907038313.$$

Thus, we have

$$n = 769441806122148057459179536286394989745390123859123728821896 0$$
$$7348911203119177173949267888201712263661991232457777858219024478 5$$
$$4995757079440397354833472303.$$

The number

$$q = 4p_1p_2 - 1 = 307776722448859222983671814514557995898156 0$$
$$4954364949152875842939564481247670869579707155280684905 4$$
$$6479649298311114328760979141998302831776158941933388921 1$$

is a prime. Since $q \equiv 3 \pmod{4}$, the elliptic curve E defined by the equation $y^2 = x^3 + x$ over $\mathbb{F}_q$ is superesingular. The point $P = (x(P), y(P))$, where

$$x(P) = 249234383028791030415509337688738175538158590076636972230312 49$$
$$1954089508938594293101431086136135995118826706761382555145184472$$
$$1968912075227277234164947109 7$$

and

$$y(P) = 737996997348676496665860701704072193490435615382792210827517600$$

$$538539755358116422263315026068694342336247347797913210910621732098503146107614456038383100$$

has order $n = p_1 p_2$.

We take $g = 2$,

$$a = 2^{256} + 2^9 + 1 = 115792089237316195423570985008687907853269984665640564039457584007913129640449$$

and

$$b = 2^{128} + 2^{100} + 1 = 340282368188589063691604008928471416833.$$

We have

$$r = 2^b \bmod n = 606047383118041902800252754427446666920498361093194816304433724860363356158421874694524415267112284647646590300127020573917994700502444986860669431119564,$$

$$2^a \bmod n = 301703278105984612331959909384645579259838330058887560280981123219109766727075670625596418215524163955319907854573382245426564094874852045289557121519086,$$

and

$$2^{a(1-b)} \bmod n = 690123530133273230626309389424846277148918273893781109989393552397526184662868089706541469966831703048453509930121476438921649862265355773278725114764186,$$

We consider the points $Q = 2^a P = (x(Q), y(Q))$, where

$$x(Q) = 726024894374351041059707058043918662331259099369849728294069637160518521744775478357470740469666592292829111355206667689244366615968601129874346167442208,$$

$$y(Q) = 180478952381617534858771173117408315328111949924113880217933526940905063141367510816973388622683154804772889445776154435381749237197181859159816306357617982,$$

and $R = 2^{a-ab} P = (x(R), y(R))$, where

$$x(R) = 101511866894396545670585188239649151557179669727386321855694497591433958158555098408768620625614580819753284158039188667649129712719578441421966525215388402,$$

$$y(R) = 118306095688161874550646029575329976723454038037424706221632110504264075261475034768741284893776696048730660200567015539148455811330398091422405264826631372.$$

Therefore $(2, P, Q, R, r, n)$ and (a, b, p_1, p_2) are a public key and the corresponding private key for our signature scheme. Moreover, we can use the Tate pairing with the distorsion map $\phi(x, y) = (-x, iy)$ with $i^2 = -1$.

8. Conclusion

In this paper we defined a signature system based on two difficult arithmetic problems. In the framework chosen, these problems have similar resistance to known attacks. We explained how to implement in practice all the basic functions we need for the establishment and operation of this system. This strategy has an interest in any application that includes a signature to be valid for long. Indeed, it is hoped that if any of the underlying problems is broken, the other will still be valid. In this case, the signature should be regenerated with a new system, without the chain of valid signatures being broken.

References

[1] P. S. L. Barreto, S. D. Galbraith, C. Ó'hÉigeartaigh and M. Scott, Efficient pairing computation on supersingular Abelian varieties, *Des. Codes Crypt.,* 42 (2007), 239-271

[2] E. Biham, D. Boneh and O. Reingold, Breaking generalized Diffie-Hellman is no easier than factoring, *Information Processing Letters,* 70 (1999), 83-87.

[3] D. Boneh, B. Lynn and H. Shacham, Short Signatures from the Weil Pairing, Lecture Notes in Computer Science 2248 (2001), 514-532.

[4] R. Bróker, Constructing Supersingular Elliptic Curves, *Journal of Combinatorics and Number Theory,* 1(3), (2009), 269-273.

[5] J. Buchmann, A. May and U. Vollmer, Perspectives for cryptographic long term security, *Communications of the ACM,* 49(9), (2006), 50-55.

[6] T.-H. Chen, W.-B. Lee and G. Horng, Remarks on some signature schemes based on factoring and discrete logarithms, *Applied Mathematics and Computation,* 169 (2005), 1070-1075.

[7] S. D. Galbraith and V. Rotger, Easy Decision Diffie-Hellman Groups *LMS J. Comput. Math.* 7 (2004), 201-218.

[8] L. Harn, Enhancing the security of ElGamal signature scheme, *IEE Proc.- Computers and Digital,* 142(5) (1995), 376.

[9] D. R. Heath-Brown, Almost-primes in arithmetic progressions and short intervals, *Math. Proc. Cambridge Phil. Soc.,* 83 1978), 357-375.

[10] F. Hess, N. P. Smart and F. Vercauteren, The Eta Pairing Revisited, *IEEE Transactions on Information Theory,* 52(10) (2006), 4595-4602.

[11] A. Joux, The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey), ANTS 2002, Lecture Notes in Computer Science 2369, pp 20-32, Springer-Verlag 2001.

[12] T. Icart, How to Hash into Elliptic Curves, CRYPTO 2009, Lecture Notes in Computer Science 5677, pp. 303-316, Springer-Verlag 2009.

[13] G. Karagiorgos and D. Poulakis, Efficient Algorithms for the Basis of Finite Abelian Groups, *Discrete Mathematics, Algorithms and Applications,* 3(4),(2011) 537-552.

[14] N. Y. Lee, Security of Shao's signature schemes based on factoring and discrete logarithms, *IEE Proc.- Computers and Digital Techniques,* 146(2), (1999), 119-121.

[15] N. Y. Lee and T. Hwang, The security of He and Kiesler's signature scheme, *IEE Proc.- Computers and Digital,* 142(5), (1995), 370-372.

[16] J. Li and G. Xiao, Remarks on new signature scheme based on two hard problems, *Electron. Lett.,* 34(25) (1998), 2401.

[17] J. S. Maseberg, Fail-safe konzept fur public-key infrastrukturen, Thesis, Technische Universitat Darmstadt 2002.

[18] K. S. McCurley, A key distibution system equivalent to factoring, *J. Cryptology,* 1, (1988), 95-105.

[19] Z. Shao, Security of a new digital signature scheme based on factoring and discrete logarithms, *International Journal of Computer Mathematics,* 82(10), (2005), 1215-1219.

[20] E. Verheul, Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems, Advances in Cryptology-Eurocrypt '01, Lecture Notes in Computer Science 2045, 195-210, Springer-Verlag 2001.

[21] S. Vladut, Cyclicity statistics for elliptic curves over finite fields, *Finite Fields and Their Applications,* 5(1), (1999), 13-25.

[22] C.-A. Zhao, D. Xie, F. Zhang, J. Zhang and B.-L. Chen, Computing bilinear pairing on elliptic curves with automorphisms, *Des. Codes Cryptogr.,* 58, (2011), 35 - 44.
[23] S. Wei, A new digital signature scheme based on factoring and discrete logarithms, Progress on cryptography, Kluwer Internat. Ser. Engrg. Comput. Sci. 769, pp. 107-111, Kluwer Acad. Publ, Boston, MA 2004.

Department of Mathematics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece
E-mail address: poulakis@math.auth.gr

Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France
E-mail address: robert.rolland@acrypta.fr